

**APPLICATION FOR UNITED STATES LETTERS PATENT**

by

**DONALD C. KAUFFMAN**

**AND**

**EDWARD S. ANDERSON**

for an

**IN-FLIGHT COMMUNICATIONS SYSTEM**

Attorney Docket No.: H0005297

## IN-FLIGHT COMMUNICATIONS SYSTEM

[0001] This application claims the benefit of U.S. Provisional Application No. 60/457,598, filed March 27, 2003, which is expressly incorporated herein by reference in its entirety.

### **BACKGROUND**

#### Field of the Invention

[0002] The present invention relates to improvements in communications systems. More particularly, the present invention relates to an in-flight communication system that allows users to send and receive messages in an inconspicuous manner, which is especially desirable for personnel, such as airline security Air Marshals, who expect to remain discrete.

#### Background of the Invention

[0003] In recent years, Air Marshals have become more prevalent on commercial airlines in view of the increased security measures necessitated by the threat of terrorism and general increased desire for public safety. To be effective, Air Marshals should preferably be able to communicate with each other, with the flight deck and/or with their command and control centers on the ground. All of these types of communication should preferably be possible from any seat on the aircraft, or indeed, from virtually any place on the aircraft. Also, any data communication should preferably be transmitted in a secured and covert mode. Heretofore, however, systems have not been fielded that embody these capabilities, let alone in a comprehensive and seamless manner. Accordingly, there remains a need to provide improved in-flight communication capabilities.

## **BRIEF SUMMARY OF THE INVENTION**

[0004]           The present invention provides a substantially comprehensive and seamless system for in-flight communications by leveraging existing technology in a manner not previously contemplated. Specifically, the present invention provides a system whereby an Air Marshal, for example, traveling on an air transport aircraft almost anywhere in the world can communicate with ground operations personnel to, e.g., report an onboard incident or receive information from the ground that is critical to his mission. The present invention also enables the Air Marshal to communicate with other Air Marshals that may be onboard the same aircraft, as well as to communicate with the aircraft flight deck officers and the cabin crew. Significantly, the system of the present invention is preferably configured such that the Air Marshal can send and receive messages in an inconspicuous manner, thereby protecting his undercover status.

[0005]           While the present invention finds particular utility in connection with airline safety and security by providing secure and covert communications capabilities to personnel such as Air Marshals, the present invention can also be used by airlines for operational efficiency. For example, cabin crews can use the system to communicate with their ground operations centers to request cabin maintenance actions or consumable replenishments at a next stop, or request/receive connecting gate information.

[0006]           In a preferred embodiment, the present invention comprises an Air Marshal terminal, such as a Personal Digital Assistant (PDA) device (e.g., a Palm Pilot) with a wireless modem, a Communication Management Unit (CMU), access to the Aircraft

Communications Addressing and Reporting System (ACARS), and a ground host.

The ACARS and ground hosts are presently available and well-known to those skilled in the art, and exist on commercial airlines and through service providers such as ARINC. The present invention leverages these facilities by layering thereon secure communications using an encryption scheme that encrypts the data transmissions, and providing a wireless network installed on the aircraft. The wireless network preferably operates in accordance with a commercial standard such as IEEE 802.11(b).

[0007] In operation, an Air Marshal, or other user, operates his PDA in a conventional manner, at least to those who may casually see such use. However, in accordance with the present invention, the PDA includes a wireless modem via which the PDA can communicate with the on-board wireless network that operates in conjunction with the CMU, which in turn, is in communication with ACARS, thereby providing ground connectivity, as well connectivity to other similarly-configured PDAs and to flight deck personnel.

[0008] The foregoing and other features of the present invention and the attendant advantages thereof will be more fully understood upon reading the following detailed description in conjunction with the accompanying drawings.

#### **BRIEF DESCRIPTION OF THE DRAWINGS**

[0009] Figure 1 depicts an exemplary network architecture for implementing a communication system in accordance with the present invention.

[0010] Figures 2 and 3 depict exemplary screen shots of a PDA configured to operate in a communication system in accordance with the present invention.

## DETAILED DESCRIPTION OF THE INVENTION

[0011] Referring to Figure 1, the present invention preferably comprises an Air Marshal terminal 101, such as a personal digital assistant (PDA) device (such as a Palm Pilot) with a wireless modem, a Communication Management Unit (CMU) 105, part of the Aircraft Communications and Addressing Routing System (ACARS) 109, and a ground host 113. ACARS 109 and ground host 113 are presently available and well-known to those skilled in the art, and exist on commercial airlines and via service providers such as ARINC. The present invention leverages these facilities by layering thereon secure communications using an encryption scheme that encrypts the data transmissions, and providing a wireless network installed on the aircraft. The wireless network preferably operates in accordance with a commercial standard such as IEEE 802.11(b). Encryption technology is well-known in the art and will not be described herein, except to note that any level of encryption may be implemented that can be supported by the available bandwidth through ACARS/ARINC or any other protocol or service over which data generated by the present invention is carried.

[0012] The use of wireless PDA 101 by an Air Marshal allows the officer (or any authorized user) to blend with the other passengers and not call undue attention to himself. Use of wireless PDA device 101 also allows the officer to roam anywhere in the cabin and maintain secure communication links. Using custom drop down menus (examples of which are shown in Figures 2 and 3), the officer can quickly send secure communications to the flight deck, other Air Marshals on the aircraft and to his command center, as well as receive secure data from the command center, other Air

Marshals, and the pilots. Security for communications is particularly desirable due to the following threats:

- ACARS messages are readable while in transit
- Messages provide identification, location and time
- “Bogus” messages can be transmitted and appear to be legitimate
- Valid messages may be altered before delivery
- Permits one entity to assume the role of another and engage in communications
- Limitations in addressing may result in delivery of message to wrong recipient

[0013] Air Marshals communications requirements that are met by the present invention include communications between an Air Marshal and Ground Operations. Such communication might include, for example, information regarding an incident on a given aircraft, or incidents on other aircraft that is relayed to the Air Marshal. The present invention also provides an Air Marshal the ability to communicate with other Air Marshals on the same aircraft, flight deck officers and other cabin crew. Such communication allows for better coordination on responses to onboard situations.

[0014] In view of the use of ACARS, the present invention further allows an Air Marshal to have air to ground communication coverage along all, or substantially all, air transport routes. In addition, the system in accordance with the present invention provides inconspicuous operation and “information assurance” in the sense that there is provided Secure (Encrypted) Communications, Authenticated Communications and Message Integrity.

[0015] Referring again to Figure 1, the present invention preferably comprises an electronic system that is composed of both hardware and software. Significant components of the system include: (1) personal digital assistant (PDA) 101 with a wireless communications transceiver (not shown); (2) a cabin wireless local area network (LAN) unit (CWLNU) (not shown); (3) a communications management unit (CMU) 105 or communications management function (CMF) software with Secure ACARS and/or ATN Security functionality; (4) a cockpit display unit and printer (not shown); (5) at least one of a VHF data link 121, HF data link 123, and/or SATCOM data link 125; (6) an ACARS, ATN, and/or future aeronautical data link network 109; and (7) a ground system 113 connected to data link network 109, and having at least one display terminal 133. By combining these components as described in more detail below, an Air Marshal can communicate from virtually any location on an aircraft 107 via wireless PDA 101 through an aeronautical data link 109 with worldwide coverage in a secure and inconspicuous manner, thereby protecting the undercover nature of the Air Marshal's mission.

[0016] Figure 1 depicts an exemplary network architecture for implementing a system in accordance with the present invention. At a high level the present invention provides, in one embodiment, an aircraft security envelope 2 that incorporates a wireless LAN that is in communication with an ACARS security envelope 4, which is in turn, in communication with, e.g., a Transportation Safety Administration (TSA) security envelope 6. As shown, the system comprises:

[0017] (1) Personal digital assistant (PDA) 101 with the wireless (IEEE 802.11) transceiver. This is a commercially available product that is preferably configured

with custom software to manage message entry display pages as well as display information sent from other users within the system. Multiple PDAs 101 can be used in the system for other users such as other Air Marshals and the cabin crew.

[0018]           (2) Cabin wireless local area network (LAN) unit (CWLNU) serves as an access point for wireless (IEEE 802.11) transmissions and converts them into, e.g., an Ethernet format, which is the interface into the communications management unit (CMU) 105.

[0019]           (3) CMU 105 preferably includes Secure ACARS software and/or ATN Security software and is preferably integrated with a basic CMU that further includes the capability of providing data security for all air - to - ground data link messages. The Secure ACARS software preferably provides, using known techniques, the security services of confidentiality (encryption), data authentication, and data integrity. Those skilled in the art will appreciate that a CMU is not critical to the present invention and is used herein only to show an exemplary implementation. For example, communications systems are presently being fielded that do not necessarily rely on the functionality of a CMU. For instance, a direct satellite link is one type of system that might bypass the CMU. Similarly, an airphone system that communicates directly with ground stations (and bypasses a CMU) could also be employed in connection with the present invention.

[0020]           (4) In a preferred implementation, CMU 105 interfaces to cockpit displays and printers which serve as communication terminals for the flight deck officers, as well as to a VHF data link radio (VDR) 141, HF data link radio (HFDR) 143, and



SATCOM data unit (SDU) 145 to provide connectivity to the ACARS, ATN, or future aeronautical data links.

[0021] (5) A satellite 151, Satellite Earth Station 152, VHF Ground Stations (GS) 154, HF Ground Stations 156, air-ground network 127, a data link service provider ACARS Central Processing System (CPS) 158 and a terrestrial network 159 constitute a typical data link network that provides digital message communications capability between aircraft 107 and ground users.

[0022] (6) Ground host / TSA Operation Center 113 preferably has peer Secure ACARS software to provide the complementary data security service as performed in CMU 105 with Secure ACARS.

[0023] (7) Finally, computer workstations 133 along with TSA Operations Center 113 permit ground personnel to send and receive communications to and from the airborne Air Marshals.

[0024] Since the Air Marshal is provided a Communications Terminal that is preferably in the form of a wireless PDA, the Air Marshal can easily roam throughout the aircraft cabin and maintain a communications link. Such a PDA further allows the Air Marshal to blend into the passenger population, since the "terminal" looks like a typical passenger's possession. Such a terminal further enables the Air Marshal to receive and transmit easily with minimal interaction or data entry. In other words, PDA 101, as used in the context of the present invention, gives an Air Marshal anonymity and roaming, both of which are significant components of mission success.

[0025] Figures 2 and 3 are exemplary screen shots of possible displays that can be presented to an Air Marshal on his PDA. Figure 2 depicts exemplary screens that are particularly suited to Air Marshal duties. These screens list types of incidents and other information about evolving emergency scenarios. In a preferred implementation, the screens are advantageously arranged to require only simple tap and click functionality, thereby freeing the Air Marshal from excess work.

[0026] Figure 3 depicts exemplary screen shots that could be presented on PDA 101 when the system of the present invention is used to augment or enhance existing flight operations capabilities. In the case shown in Figure 3, the screens show flight information and flight schedule information provided, e.g., by a particular airline.

[0027] As those skilled in the art will appreciate, there are tradeoffs in selecting the type of terminal that an Air Marshal might use. There are two basic choices: Data (e.g., a PDA) or Voice.

[0028] The following characteristics are associated with a PDA (Data Communication):

- Preformatted data entry screens allows for quick and complete standard messages
- Ability to uplink and downlink messages and graphics
- Multiplex use of existing aircraft data link equipment
- Worldwide coverage
- Ground system required at headquarters for messaging

[0029] The following characteristics are associated with Voice Communication:

- Not as discrete as text messaging
- Easily overheard – Draws attention to Air Marshal
- Unable to graphically convey the situation

- Requires a dedicated voice channel from aircraft
- Additional radio and antenna on aircraft
- Additional spectrum / frequency allocation
- Additional ground stations

[0030] In view of the foregoing, the present invention is preferably based on data-type communication. However, to the extent voice communications can be kept discrete and be operated without significant aircraft or communication facilities modifications like those mentioned above, the present invention can also be augmented to support speech capabilities. Further, in view of the use of a PDA, wireless airborne network and air-to-ground connectivity consistent with the principles of the present invention, information assurance is provided in the forms of:

- Data Authentication — Provides strong authentication of the terrestrial and airborne communicating peer entities
- Data Integrity — Provides end-to-end data integrity for the payload in uplink and downlink messages
- Confidentiality — Provides end-to-end data confidentiality for the payload in uplink and downlink messages

[0031] Likewise, the present invention provides cryptographic strength by preferably implementing cryptographic algorithms and key length(s) suitable for protecting civilian “For Official Use Only” (FOUO) and military “Sensitive-But-Unclassified” (SBU) data.

[0032] With reference to Figure 1, the flow of a typical Air Marshal communication message is as follows:

#### Message Uplink

- Ground user composes message to aircraft

- Secure ACARS Ground System protects message at TSA Operations Center
- Protected message transits terrestrial networks to ACARS Data Link Service Provider
- Protected message transits DSP ground – ground and air-ground networks to aircraft
- CMU authenticates ground user, decrypts message, forwards to Air Marshal via protected IEEE 802.11 message, and displays message on flight deck Multi-function Control and Display Unit (MCDU), if authorized
- PDA or any other portable device receives, via CMU 105, IEEE 802.11 message and decrypts for user
- PDA or other portable device alarms / notifies user of incoming message

#### Message Downlink

- Air Marshal composes message on PDA using predefined message structure or free text entries
- PDA transmits protected IEEE 802.11 message to CMU
- CMU encrypts message, transmits message via ACARS network, and displays message on flight deck Multi-function Control and Display Unit (MCDU), if authorized
- Protected message transits ACARS air - ground and ground - ground networks to DSP
- DSP forwards protected message to TSA Operations Center via ground - ground network
- Operations Center authenticates Air Marshal and decrypts message

[0033]           Those skilled in the art will appreciate that while the function of encrypting and decrypting is performed by the CMU, the PDA device itself could also perform

these functions as long as the appropriate keys and processing power were available to the device.

[0034] In view of the architecture and components employed in a system in accordance with the present invention, it is possible to significantly, if not completely, eliminate the following threats that Air Marshals and their colleagues face:

- Disclosure - Messages are readable while in transit
- Traffic Analysis - Messages provide identification, location, and time
- Spoofing - Bogus messages can be transmitted and appear to be legitimate
- Modification - Valid messages may be altered before delivery
- Masquerade - Permits one entity to assume the role of another entity and engage in communications
- Mis-delivery - Limitations in addressing may result in delivery of messages to wrong recipient

[0035] The foregoing disclosure of the preferred embodiments of the present invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many variations and modifications of the embodiments described herein will be apparent to one of ordinary skill in the art in light of the above disclosure. The scope of the invention is to be defined only by the claims appended hereto, and by their equivalents.

[0036] Further, in describing representative embodiments of the present invention, the specification may have presented the method and/or process of the present invention as a particular sequence of steps. However, to the extent that the method or

process does not rely on the particular order of steps set forth herein, the method or process should not be limited to the particular sequence of steps described. As one of ordinary skill in the art would appreciate, other sequences of steps may be possible. Therefore, the particular order of the steps set forth in the specification should not be construed as limitations on the claims. In addition, the claims directed to the method and/or process of the present invention should not be limited to the performance of their steps in the order written, and one skilled in the art can readily appreciate that the sequences may be varied and still remain within the spirit and scope of the present invention.